

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

CR. NO. 20-20594

v.

HON. DENISE PAGE HOOD

AMIN HASANZADEH,

Defendant.

_____ /

MOTION TO DISCLOSE AND SUPPRESS FISA MATERIALS

There are four categories of discovery Amin Hasanzadeh believes are in the government's possession and material to his defense. The first three categories are mentioned in Hasanzadeh's motion to compel: (1) any authorization to search his ex-wife's University of Michigan email account, (2) any authorization to search his residence prior to November 6, 2019, and (3) any authorization for recordings of private phone calls. Hasanzadeh has not received documentation of the government's legal authority for conducting these portions of its investigation. Fourth, the government produced a hard drive containing the contents of 10 devices seized as part of the investigation into Hasanzadeh, but it has declined to provide information about when these devices were seized or where they were seized.

The government does not deny that these materials are in their possession and are material to Hasanzadeh's defense. Instead, the government suggests (without explicitly stating) that the materials were secured pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended by 50 U.S.C. §§ 1801, 1802. (*See* R. 72, Gov. Resp. Mtn. Compel, PgID 579.) The government states that, if Hasanzadeh wants FISA materials, he must move for disclosure under 50 U.S.C. §§ 1806 and 1825.

Accordingly, for the reasons in the attached brief, Hasanzadeh moves under 50 U.S.C. § 1806(e) for disclosure of FISA materials and to suppress all information unlawfully acquired or surveillance conducted not in conformity with an order of authorization or approval, and to suppress any fruits of unlawful surveillance or searches.

Respectfully submitted,

FEDERAL COMMUNITY DEFENDER

/s/ David C. Tholen

/s/ Benton C. Martin

Attorneys for Defendant

613 Abbott Street, Ste. 500

Detroit, Michigan 48226

E-mail: david_tholen@fd.org

Date: February 11, 2022

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

CR. NO. 20-20594

v.

HON. DENISE PAGE HOOD

AMIN HASANZADEH,

Defendant.

_____ /

**BRIEF IN SUPPORT OF
MOTION TO DISCLOSE AND SUPPRESS FISA MATERIALS**

Amin Hasanzadeh seeks (1) any authorization to search his ex-wife's University of Michigan (UM) email account, (2) any authorization to search his residence prior to November 6, 2019, and (3) any authorization for recorded telephone calls. In addition, Hasanzadeh has received a hard drive from the government containing the contents of 10 electronic devices, but has not been told where any of the devices were seized or when. The government has suggested, without explicitly saying, that FISA prevents disclosure.

Hasanzadeh has good reason to believe that these materials exist and are material to his defense. As to the UM email account of Fatemah "Noyan" Akbar (Hasanzadeh's ex-wife), the defense has received an FBI report indicating: "On 7/20/2017, FBI DE served a secondary warrant on the University of Michigan for

noyan@umich.edu.” This warrant was based on previous investigation showing that Akbar’s University of Michigan cloud storage drive housed documents from Hasanzadeh’s former employer. The documents obtained through these searches of Akbar’s University of Michigan account—which the government has alleged Hasanzadeh used as well—appear to have served as critical background for the further investigation of Hasanzadeh’s alleged crimes. The defense has received no documentation of the legal authorization for these searches.

Second, at least one physical search of Hasazadeh’s residence occurred before November 1, 2019. On that day, Magistrate Judge Mona Mazjoub issued a search warrant for which probable cause was based, in part, on a prior “covert” search of Hasanzadeh’s residence. The warrant affidavit explains:

In December 2017, the FBI, pursuant to Court authorized process, surreptitiously entered HASANZADEH’s former residence in Ann Arbor, Michigan where he lived with Person A. The surreptitious entry revealed that Person A and HASANZADEH owned, maintained, and utilized numerous electronic devices, to include three laptop computers However, these items were not seized by the FBI as part of the covert search.

Investigative analysis of these laptop computers, which remained at HASANZADEH’s former Ann Arbor residence after the surreptitious search, revealed the existence of thousands of confidential files belonging to Victim Company A, many of which were discussed above. These files were identified as, but not limited to, internal company component lists, schematics, diagrams, and other project reports marked as confidential. . . .

The defense has received no documentation of the legal authorization for this “surreptitious search.”

Third, as to recorded telephone calls, the government has produced transcriptions of conversations between Hasanzadeh, his wife Akbar, and his brother. But the government has not provided documentation of the legal authorization for listening to or recording these phone calls.

If federal agents used illegal methods to investigate Akbar's UM account, Hasanzadeh's residence, or private phone calls, then the fruits of those illegal searches would be subject to suppression. The government has provided notice of their intent to use foreign intelligence surveillance information at trial. (R. 49, Notice, PgID 194.) This notice simply informed the defense that the government has FISA evidence, but provided no details regarding the reasons for the national security surveillance. It was not clear to the defense until litigation of the motion to compel that the specific items Hasanzadeh seeks are covered by FISA, and the government has not explicitly said so even now.

Congress enacted FISA in response to perceived abuses of intelligence gathering and surveillance procedures by federal intelligence agencies in the early 1970s. *See American Civil Liberties Union v. Clapper*, 785 F.3d 787, 792–93 (2d Cir. 2015). The defense moves to discover all evidence, intelligence, counter-intelligence, FISA applications, FISA orders, and all information concerning surveillance of Hasanzadeh, and the national security justification for all governmental actions concerning Hasanzadeh.

ARGUMENT

FISA “is not to be used as an end-run around the Fourth Amendment’s prohibition of warrantless searches.” *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991). Thus, when a defendant moves for discovery and suppression of FISA materials, the Court must engage in a careful, detailed examination of whether the government complied with the law in obtaining FISA-covered evidence. As part of this process, the Court may disclose these materials to the defense if, without defense input, it “is unable to make an accurate determination as to the legality of the evidence.” *United States v. Daher*, No. 18-20559, 2020 WL 7664789, at *2 (E.D. Mich. Dec. 24, 2020).

Under 50 U.S.C. § 1806(f), the government may invoke an in camera, ex parte process for review of FISA materials. Under that process, “if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States,” then this Court reviews “in camera and ex parte” any “materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved was lawfully authorized and conducted.” *Id.* “In making this determination, the court may disclose to the aggrieved person [here, Hasanzadeh], under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only

where such disclosure is necessary to make an accurate determination of the legality of the surveillance.” *Id.*

“Section 1806(f) vests sole authority to hold legality hearings in a district court.” § 9:48. Ex parte, in camera determination, 2 Law of Electronic Surveillance § 9:48. If the Attorney General does not file an affidavit as discussed above, then discovery must proceed in a standard manner. *Id.* “In determining whether disclosure is necessary, the Court should consider whether, after its initial review, any irregularities are revealed, such as whether: the materials evidence a possible misrepresentation of fact; the persons to be surveilled are not clearly identified; or the surveillance records include a significant amount of nonforeign intelligence information, indicating a possible issue with the minimization standard utilized.” *United States v. Mahamud*, 838 F. Supp. 2d 881, 885 (D. Minn. 2012).

There are multiple questions the Court must answer in reviewing these materials. For example, the following is a non-exhaustive list of issues the Court must examine in reviewing the materials:

First, the Court must determine whether the primary purpose of the surveillance was “*domestic* criminal activity, which is not authorized by FISA.” *United States v. Daoud*, 761 F.3d 678, 682 (7th Cir. 2014). “Although evidence obtained under FISA subsequently may be used in criminal prosecutions, the

investigation of criminal activity cannot be the primary purpose of the surveillance.”

United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991) (citation omitted).

Second, this Court must review whether the FISA application complied with the requirements for such applications, which “must contain, among other things, a certification that the purpose of the requested surveillance is the gathering of foreign intelligence information and a detailed description of the nature of the information sought.” *Johnson*, 952 F.2d at 572. This review includes examining whether the government properly certified that the information sought through the FISA process could not “reasonably be obtained by normal investigative techniques.” 50 U.S.C.A. § 1823. It also includes examining whether the government conducted its surveillance in accordance with minimization procedures FISA requires. 50 U.S.C. § 1823(a)(3).

Third, the Court must decide whether any FISA warrants or applications were supported by probable cause: “Like any search warrant, a FISA application must be supported by probable cause.” *Daoud*, 761 F.3d at 681. This probable cause determination differs from the standard analysis this Court undertakes because it focuses on whether Hasanzadeh was an “agent of a foreign power.” *Daher*, 2020 WL 7664789, at *4. FISA also demands particularity: The government must show whether “each of the facilities, places, premises, or property at which the electronic

surveillance or physical search was directed was, or was about to be owned, used, possessed by, or was in transit to or from [Hasanzadeh].” *Id.*

Fifth, even assuming the government needed to use the secret FISA process initially, this Court must determine whether that need for secrecy still exists. *See United States v. Warsame*, 547 F. Supp. 2d 982, 989 (D. Minn. 2008).

These are complicated questions, and questions that should be decided with defense input in this case. Hasanzadeh thus requests that, pursuant to this procedure, this Court review and disclose any FISA applications, FISA orders, and FISA materials under appropriate security procedures and protective orders. Hasanzadeh further requests a copy of the Attorney General’s affidavit attesting that disclosure of evidence would harm national security.

This case echoes concerns raised by Congress, when it authorized changes to FISA in 2001, that “‘it will be up to the courts to determine how far law enforcement agencies may use FISA for criminal investigation and prosecution *beyond* the scope of the statutory definition of ‘foreign intelligence information.’” *In re Sealed Case*, 310 F.3d 717, 733 (Foreign Int. Surv. Ct. Rev. 2002) (quoting Senator Leahy, 147 Cong. Rec. S11004 (Oct. 25, 2001)). This Court should authorize and compel disclosure of the FISA applications and orders in this case, especially any FISA surveillance that resulted in evidence used to establish probable cause for later non-FISA searches.

CONCLUSION

Under 50 U.S.C. § 1806, this Court should do the following:

1. Compel the government to determine if the Attorney General will submit an affidavit attesting that disclosure of FISA applications, FISA orders, and other FISA materials in this case would harm national security;
2. Provide Hasanzadeh a copy of the Attorney General affidavit, if filed;
3. Conduct an in camera, ex parte inspection, review of any FISA applications, FISA orders, and FISA materials, and determine whether the surveillance was lawfully authorized and appropriately conducted;
4. Disclose any FISA applications, FISA orders, and FISA materials to defendant's counsel because such disclosures are necessary to make an accurate determination of the legality of the surveillance; and
5. Suppress all information unlawfully acquired or surveillance conducted not in conformity with an order of authorization or approval, and suppress any fruits of unlawfully surveillance or searches.

Respectfully submitted,

FEDERAL COMMUNITY DEFENDER

/s/ David C. Tholen

/s/ Benton C. Martin

Attorneys for Defendant

613 Abbott Street, Ste. 500

Detroit, Michigan 48226

E-mail: david_tholen@fd.org

Date: February 11, 2022

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

CR. NO. 20-20594

v.

HON. DENISE PAGE HOOD

AMIN HASANZADEH,

Defendant.

_____ /

CERTIFICATE OF SERVICE

I certify that on February 11, 2022, I electronically filed the foregoing paper with the Clerk of the Court using the ECF system which will send notification of such filing to all parties of record.

s/ Benton C. Martin
Federal Community Defender Office